京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学
KYOTO UNIVERSITY

Title	チャールズ・バベッジ"Cypher Writing"について (数学史の研究)
Author(s)	野村, 恒彦
Citation	数理解析研究所講究録 (2009), 1625: 120-130
Issue Date	2009-01
URL	http://hdl.handle.net/2433/140294
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

数理解析研究所講究録
第1625巻 2009年 120-130

チャールズ・バベッジ“Cypher Writing”について

兵庫県社土木事務所　野村　恒彦 (Tsunehiko Nomura)
Yashiro Public Construction Office of Hyogo Prefecture

はじめに

暗号とは、「メッセージの外見を変えることにより、正当な受信者にしか読めないようにする方法のこと[*1]」とされる。暗号の研究は数学的見地から視点ももちろん考えることができるが、19世紀ではその軍事的重要性も非常に大きなものとなっていた。

チャールズ・バベッジは暗号にも興味を持っており、それは*Journal of Society of Arts*においてスウエーツ(J. H. B. Thwaites)との書簡があることや、自伝でも暗号解読について書かれた節が設けられていることからも理解できる。

ここでは、バベッジによる書簡や自伝の記述に基づきバベッジの暗号への興味がどのようなものであったかを考え、またその時代背景からも暗号の意義について考えてみることにしたい。

また、本発表にかかる先行研究は、シン(参考文献[8])及びフランクセン(参考文献[5]、[6])がある。

1　暗号について

(1) 暗号の歴史について

暗号は単純なものから始まっているが、その代表的なものは単一換字式と呼ばれる。これは例えばアルファベットを数文字ずらすことにより暗号化するというものである。しかし、暗号としては非常に単純な構造なので容易に解読されてしまう欠点を持っている。これを改良したものが、平方換字式と呼ばれるヴィジュネル暗号である。ヴィジュネル暗号はフランスの外交官であるブレーズ・ド・ヴィジュネル(Blaise de Vigenère)が考案し、1586年に『秘密の書記法について』(*Traicte des Chiffres*)により発表したものであり、これについては後に詳述する。

既に述べたように、暗号は非常に重要な情報を関係者以外に読むことができないようにして伝達する手段であり、その性質上国家機密（特に軍事的機密）を扱うために改良がなされていたと考えられる。事実ヴィジュネルが暗号を発表した時代では、ユグノー戦争(1562～1598)が起こっていた。本稿で述べるバベッジとスウエーツの書簡が交わされた時代でもクリミア戦争(1854～1856)が勃発しており、暗号に対する関心が高まっていたことは想像に難くない。

現代にあっては、インターネット等において個人情報の伝達等に暗号が利用されていることは周知のとおりである。一方、探偵小説でも暗号を題材とするものがあり、具体的な作品として E・A・ポー,の「黄金虫」(“Gold Bug”)や、A・C・ドイル,「踊る人形」(“The Adventure of Dancing Men”)がある。

(2) 数学との関連

古くから科学者が自身の研究の先取権を確保するために、研究の内容を他人にはわからないような手段で記述していたことが知られている。しかし、これは記述者個人にしか理解できないので、伝達を目的とした暗号とは異なるものと考えることができる。

また次節でも述べるように、暗号や暗号解読については軍事的機密とも大きく関係しており、その理論は数学と大きな関係があるにもかかわらず、具体的に明らかになっているとは言い難い。ただし、第2次大戦下におけるA・チューリングによるナチスの暗号「エニグマ」の解読については著名な事実としてよく知られている。

---

*1 サイモン・シン,『暗号解読－ロゼッタストーンから量子暗号まで』, 青木薫訳, 新潮社, 2001, p.10.

2　バベッジと暗号

バベッジは自伝で「暗号解読について」(On deciphering)の節を設けて、暗号解読は最も魅力的な技術の一つであり、自分がそれに値する時間以上に時間を無駄遣いしていのではないかと恐れると自身の見解を述べている*2。またそこでは、暗号解読の要領の最も風変わりな特徴の一つは、普通程度に暗号解読に精通した人でさえ各人が持っている、誰も解読することできない暗号を作成できるという強い信念であるとも延べ、さらにより独創的な人であればあるほど、その人がもつ暗号に関する信念に、より密接な関係があると言及している*3。これは暗号作成や解読の技術において、個人の個性の影響下にあるということを意味している。さらに自伝では王立協会の会長であったデイヴィーズ・ギルバート(Davies Gilbert)や、バベッジの友人であるフィットン(William Henry Fitton)との間で交わされた暗号解読についてのエピソードを紹介している。

しかし、ここではスゥエーツとの間で意見交換がなされた“Correspondence of Cypher Writing”について延べ、続いて“Cypher Writing”について述べることにするが、その前にバベッジの業績との関連について述べておきたい。

スゥエーツとの書簡が交わされた当時のバベッジの主な業績には次のようなものがあるが、ここでも関心の対象は多岐にわたっている。

1851年　*The Exposition of 1851*
1853年　“On the Statistics of Lighthouses”
1855年　“Submarine Navigation”
“On the Possible Use of the Occulting Telegraph at Sebastopol”
“Note on the Swedish Machine of Messrs. Scheutz to Calculate Mathematical Tables by Method of Differences, and to Print the Results on Stereotype Plates”

これらは、ロンドンで開催された万国博覧会の全貌を紹介するものや、灯台のランプの点滅や潜水艦の航行に関するものである。特に最後のものは、スウェーデンの技術者であるシュルツが作成した階差エンジンについて書かれたものである。従って、この時期にバベッジが暗号解読に関して興味を集中していたとは考えにくく、あくまでもバベッジの関心があるテーマであったと考えることができる。

(1)　“Correspondence of Cypher Writing”について

①　概要

バベッジとスゥエーツの書簡は5通あり、1854年に*Journal of Society of Arts*に掲載された。それらは以下のようになっている。ここで“Correspondence of Cypher Writing”という題名は、著作集に収められる際に独自に付されたものである。

“Secret or Cypher Writing”	1854年90号	(スゥエーツの投稿)
“Mr Thwaites's Cypher”	1854年93号	(バベッジの投稿)
“Secret or Cypher Writing”	1854年95号	(スゥエーツの投稿)
“Mr Thwaites's Cypher”	1854年98号	(バベッジの投稿)
“Mr Thwaites's Cypher”	1854年(掲載号不明)	(スゥエーツの投稿)

これら書簡はすべてのものが著作集に収録されているわけではなく、著作集にはスゥエーツの最後の書簡を除いた4通と、後述する“Cypher Writing”を含めて5通が収録されている。フランクセンの著作*Mr. Babbage's Secret: the Tale of a Cypher – and APL*では、バベッジとスゥエーツの書簡5通と、それらに関連したカーナリー(J. B. Kearnery)の“Mr Thwaites's Cypher”が併せて収録されている*4。

---

*2 Ch. Babbage, *Passages from the Life of a Philosopher* (London: Pickering & Chatto, 1994), p.174.
*3 *Ibid.*, p.175.
*4 O. L. Franksen, *Mr. Babbage's Secret: the Tale of a Cypher – and APL* (Strandberg, 1984), pp253-8..

Journal of Society of Arts に掲載されたバベッジの書簡には、*C* との署名がなされている。*C* とバベッジが同一人物であると確かめられたのは、バベッジの自伝に自身の業績として掲げられているからである*5。しかし理由は不明であるが、バベッジの自伝の目録には本稿で述べる "Cypher Writing" が欠落している。

② 内容

スゥエーツとの書簡を順序に従って検討していくことにする。まず 1854 年 90 号に掲載されたスゥエーツからの投稿であるが、それは次のようである*6。

スゥエーツは新しい暗号を発見したと言及した(図 1)。それによれば、'I have had an interview.' は、'R BBPA OQI XW CONAYLNBF.' と暗号化されるとしている。

それに対しバベッジは 1854 年 93 号に掲載された書簡で、スゥエーツが言及した暗号は以前から使われているものであると指摘した*7。

このバベッジの書簡に対し、スゥエーツは 1854 年 95 号に掲載した書簡で、スゥエーツはこの暗号で特許を取得するつもりであることを言及し、さらに同書簡でスゥエーツはシェークスピアの「テンペスト」を独自の暗号で書いたものを掲載し、鍵となる単語(Keyword)を指摘せよと挑戦した(図 2 及び図 3)*8。

スゥエーツの挑戦に対しバベッジは 1854 年 98 号に掲載された書簡で、スゥエーツの暗号が、ヴィジェネル暗号であることを理解し、解読した*9。バベッジは書簡の中でその解読の方法を提示しているが、その方法とはヴィジュネル暗号の解読法であり、次のようなものである。

まず、表 1 のような「剰余の表」が与えられる。

Remainder	*Tabular number*	*Remainder*	*Tabular number*
0	24	12	22
1	2	13	8
2	17	14	16
3	7	15	25
4	1	16	3
5	11	17	5
6	8	18	9
7	4	19	12
8	6	20	4
9	23	21	3
10	14	22	13
11	15	23	7

表 1 バベッジによる剰余の表

次にバベッジは解読法の説明に入っているが、まず 'thou' は暗号ではgomwとhwkcとなっていることを指摘し、次のような計算を行うことを主張する。

暗号gomwにおけるgは、暗号文における142文字目にあたる。142=5×24+22となり余りは22、*Tabular number* は表により13となる。

---

*5 Babbage, *op. cit.*, p. 375.

*6 J. H. B. Thwaites,, "Secret or Cypher Writing" , *Journal of Society of Arts*, No. 90, 1854, pp.663-4.

*7 Ch. Babbage, "Mr Thwaites's Cypher" , *Journal of Society of Arts*, No. 93, 1854, pp.707-8.

*8 J. H. B. Thwaites,, "Secret or Cypher Writing" , *Journal of Society of Arts*, No. 95, 1854, pp.732-3.

*9 Ch. Babbage, "Mr Thwaites's Cypher" , *Journal of Society of Arts*, No. 98, 1854, pp.776-7.

また、gは通常のアルファベットの7番目にあたる。以上のことを前提に、次のような計算を行う。

	7　通常のアルファベットの位置
	13　*Tabular number*
最終的な余り	-6
加算	26
	20　20番目のアルファベットはtである。

この解法に従って、バベッジは鍵を TWO と COMBINED を指摘したが、その方法は完全には説明されていない。これについてはフランクセンが APL 言語を使用しての解読方法を解説している*10。フランクセンの記述でもバベッジの書簡における説明は完全にはなされていないので、それを含めて詳述することにする。またバベッジはこの書簡において、独自に「テンペスト」の文章を暗号化し、その鍵となる単語を見いだすよう逆に挑戦していることも付け加えておきたい(図4)。

③　バベッジによる解法

ヴィジュネル暗号の複雑性は、その鍵となる単語を用いて変換表が変化していくことにある。図1を例にとって説明しよう。鍵となる単語はTELEGRAPH である。第1列のKを注目すると、すぐ横にある第2列はTとなっていることがわかる。以下奇数列は第1列と同じものだが、偶数列が変化していくのである。第1列Kを横に見ていくと、第4列目はEであり、第6列目はL、以下偶数列はE、G、R、A、P、Hとなっている。これが鍵となる単語であり、第1列に該当する文字(この場合はK)も併せて示しておく必要がある。これをスウエーツは *telegraph* against K と表記している。

次に変換の方法であるが、原文の1文字を変換する場合は第1列と第2列を使う。すなわち、IはRに変換される。次に2文字目を変換する場合は第3列と第4列を使用する。これによるとHはBになる。これらからわかるように、同じ文字でもその位置により変換された文字が異なるのがヴィジュネル暗号の特色であり、最大の強みである。

さて、バベッジの暗号解読法であるが、まず原文と暗号とを比較し、原文の同じ文字が同じ文字で暗号化されているのを確かめると、24文字間隔であることがわかる。例えば原文の6文字目はiでありQとなって暗号化されているが、次にiがQと暗号化されているのは30文字目である。その間隔が24文字あるという意味である*11。

バベッジがどのようにして2つの表を用いて暗号化することを知ったかは明らかではないが（明確な根拠は見出せなかったが、当時ヴィジュネル暗号は2つの表を用いるのが通常のものであった可能性がある。)、暗号化で用いる表が2つあることは、24文字の鍵となる単語は不自然であることから容易に確かめられる。すると鍵となる単語は、24の約数の組み合わせの数を持つことが理解できる。1と24の組み合わせは、先述の理由によりあり得ないので、あと残る組み合わせは2と12、3と8、4と6であるが、3と8以外の組み合わせは12を公倍数に持つので、12文字間隔で原文の同じ文字が同じ文字で暗号化されなければならない。ここで12文字間隔を持つものはないので、3と8の組み合わせ以外に鍵となる単語の文字数はない。

次に第1の表を3文字、第2の表を8文字とする表を考えてみると、表2のようになる。ここで第2の表の同じ番号のものに注目すると（第2の表は同一の表を使うという意味である)、1文字目は第1の表の1番目の表を使用し、9文字目は第1の表の3番目の表を使い、17文字目は第1の表の2番目の表を使用していることがわかる。具体的には、1文字目Sは暗号ではUになっており(第1の表の1番目の表を使用)、9文字目NはKに(第1の表の3番目の表を使用)、17文字目RはW

*10 Franksen, *op. cit.*, pp.286-8.

*11 1組以上のものを具体的に述べると、文字間隔が24文字となっているものが18組、48文字が6組、72文字が5組、96文字が5組、120文字が4組、144文字が4組、168文字が2組、192文字が2組である。

に変換(第1の表の2番目の表を使用)されているので、これらを基に変換表を作成すると表3のようになる。すると表3で意味のある単語は、log、rum、twoの3つとなり、バベッジが書簡の中で述べている単語と一致する*12。

次に、表2において第1の表の同じ番号に着目して同様な作業を行うと表4が得られる。ここで意味をもつ単語はcombinedだけである。すると3種類の表の組み合わせが考えられることになるが、ここではtwo とcombinedの組み合わせを考えてみると表5のようになる。

さらにアルファベットを数字化して(aを1、bを2、以下zを24とする。)、原文が暗号化される過程を数値化する。すると原文の1文字目S(19文字目)が表5の左表ではt(20文字目)に変換され(+1文字)、表5の中央の表でt(20文字目)がu(21文字目)に変換される(+1文字)。同様に2文字目o(15文字目)が表5の左表ではs(19文字目)に変換され(+4文字)、表5の中央の表でs(19文字目)がf(6文字目)に変換される(+13文字)。その変換の数値化を一覧にしたものが、表5の右表になる。しかし、これはバベッジが書簡で示した表1と一致しない。

それを一致させたものが、表6である。表6では第1文字目S(19文字目)が表6の左表でw(23文字目)となり(+4文字)、w(23文字目)が表6の中央の表でu(21文字目)に変換される(+24文字)。同様に2文字目o(15文字目)が表6の左表ではv(22文字目)に変換され(+7文字)、表6の中央の表でv(22文字目)がf(6文字目)に変換される(+10文字)*13。これらを基にして作成した表6の右表は、表1と一致する。

表5と表6の相違は、twoとcombinedの位置が異なっている点である。表5ではtwoはSの位置にあり(against s)、combinedはBの位置にある(against b)のに対し、表6ではtwoはPの位置にあり(against p)、combinedはEの位置にある(against e)。後者の記述はバベッジの書簡のそれと完全に一致する*14。

バベッジによるスゥエーツが提示した暗号に対する解読がなされた後には、2通の書簡が取り交わされている。それは、スゥエーツよりの書簡(1853年10月11日付)とカーニー(J. R. Kearney)よりの書簡(1854年10月6日付)である*15。前者においてスゥエーツは書簡における C(バベッジ)の主張が良く理解できたとして感謝の意を表している。また後者においては、バベッジとスゥエーツとのやりとりを知ったカーニーが、半世紀程度以前のウィルキンス僧正が用いた暗号を紹介している。

(2) "Cypher Writing"について

① 概要

先の一連の書簡より1年後の1855年159号に掲載であり、スゥエーツの暗号には言及していないが、次に述べるように暗号に関するバベッジの考え方がよく表されている*16。

② 内容

バベッジは暗号解読というのは時間を要するものであると述べ、自身は人から暗号解読を依頼されても断るのだが、暗号解読に注目している少数の人たちに解読を依頼するのは、多くの人にとっては有益であるかもしれないと指摘する。そして解読できない暗号を考案することは重要なことではないとし、暗号はそれを使用する人によって容易にかつ迅速に書くことができなければならず、また暗号を送られた人によって容易にかつ迅速に読むことができなければならないと続

---

*12 Babbage, *op. cit.*, p.777.

*13 バベッジは書簡の中で、この暗号文の2文字目Tが誤りであり、Fが正しいことを指摘している。*Ibid.*, p.777.

*14 *Ibid.*, p.777. なお、表5でのtwo(against s)、combined(against b)でも暗号は解読できるが、ここでは表1にあわせた。

*15 Franksen, *op. cit.*, pp.257-8.

*16 Ch. Babbage, "Cypher Writing", *Journal of Society of Arts*, No. 159, 1855, pp.40-1.

けている*17。そしてその直後に、暗号解読の技術は錠前破りと似たようなところがある。数多くの錠前が破られているが、唯一の問題は、それにどれだけの時間がかかったかということであるとも述べている*18。

この“Cypher Writing”において最も注目すべきことは、バベッジは自分が解読した最近の難解な暗号は30時間を費やしたことと、過去に解読した暗号は4日もしくは5日を要したことを報告した後、フランス政府のためにパリにおいて解読した暗号には数ヶ月を必要としたことについて言及している点にある*19。先に述べたように軍事的機密の関係からか、その内容には具体的記述が全くなされていない。しかしここでわかることは、バベッジは暗号に深い興味を持ち、数多くの暗号を解読していることや、その技術の水準はフランス政府にも知られていたことである。

③ スゥエーツとの書簡の意義

バベッジとスゥエーツとの書簡の内容を吟味してみると、そこには重要な内容が含まれていることがわかる。まず、暗号が興味の対象となり得たことである。暗号は軍事的機密ばかりではなく、商取引にも使用されていたことは容易に推察され、それだけ身近なものと捉えられていたと考えることができる。

次に、ヴィジェネル暗号についての情報は行き渡っていなかったことがわかる。これは前にも述べたように軍事的機密の関係があると思われる。その複雑さと解読の困難性の認識があったためである。

そして、スゥエーツの書簡にあるように、暗号で特許が取得できたことである。

むすび

本稿で論じたように、バベッジはスゥエーツとの書簡における暗号の解読について解答(鍵となる単語)は述べているが、その方法までは全くと言って良いほど言及していない。その理由として暗号の解読方法が軍事的な重要機密として扱われ、国家がバベッジに秘匿するよう依頼したという説がある。その信憑性の根拠の一つとして、ヴィジュネル暗号が解読された時期の問題がある。ヴィジュネル暗号が解読されたのは、1863年に刊行されたF. W. カシスキーの『暗号文と解読技術』とされているが、これはバベッジのスゥエーツとの書簡より10年近く遅い*20。バベッジは明らかにヴィジュネル暗号を解読していたのだが、それを公表しなかったのは国家から秘匿依頼があったとするものである。また別の根拠として、いわゆるケンブリッジ・サークルがある。それは、政府の中枢にある人物とバベッジはケンブリッジ大学の卒業生として知己である可能性があり、その関係から秘匿依頼があったとするものである。これらはある程度信憑性があるが、事実ではないと考える。というのは、バベッジと政府との関係は、階差エンジンのプロジェクトをめぐり険悪なものであり、容易にバベッジが承諾するとは考えにくいからである。従って暗号解読は、バベッジの自伝での記述や“Cypher Writing”での言及から考えて、あくまでも数学的な興味を削ぐとして、具体的な解法を明かさなかったと考えるのが妥当である。

なお、バベッジが自伝の中で述べている暗号はヴィジュネル暗号とは異なるものであるが、これについては今後の課題としたい。

参考文献

[1] Babbage, Ch., “Mr Thwaites's Cypher”, *Journal of Society of Arts*, No. 93, pp.707-8; No.98, pp.776-7, 1854.

[2] Babbage, Ch., “Cypher Writing”, *Journal of Society of Arts*, No. 159, 1855, pp.40-1.

[3] Babbage, Ch., *Passages from the Life of a Philosopher* (London: Pickering & Chatto, 1994),

*17 *Ibid.*, p.40.

*18 *Ibid.*, p.40.

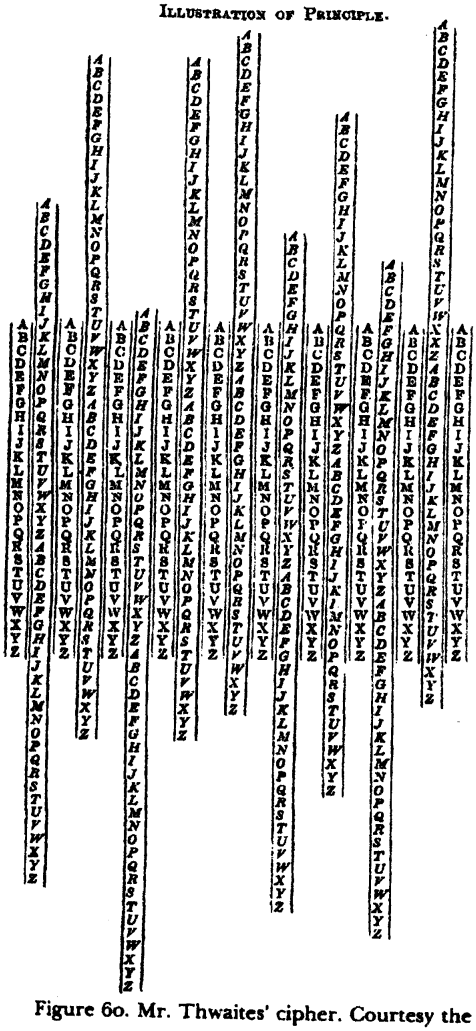
*19 *Ibid.*, p.41.

*20 シン, 前掲書, p.119.

pp.174-79.
[4] Babbage, Ch., *The Works of Charles Babbage Vol.5* (London: Pickering & Chatto, 1989).
[5] Franksen, O. L., *Mr. Babbage's Secret: the Tale of a Cypher – and APL* (Strandberg, 1984).
[6] Franksen, O. L., "The Secret Hobby of Mr. Babbage", *Systems Analysis Model Simulations*, Vol. 3, No. 2, pp.183-94.
[7] Thwaites, J. H. B., "Secret or Cypher Writing", *Journal of Society of Arts*, No. 90, pp.663-4 ; No.95, pp.732-3, 1854.
[8]S. シン,『暗号解読ーロゼッタストーンから量子暗号まで』, 青木薫訳, 新潮社, 2001, pp.100-45.
[9]F. パイパー、S. マーフィ,『暗号理論』, 太田和夫・國廣昇訳, 岩波書店, 2004, pp.1-67.
[10]E. A. ポー,「黄金虫」,『ポー小説全集 4』, 丸谷才一訳, 創元推理文庫, 1974, pp.8-59.
[11]A. C. ドイル,「踊る人形」,『シャーロック・ホームズの復活』, 大久保康雄訳, 早川書房, 1963, pp.67-98.
[12]江戸川乱歩,『続・幻影城』, 早川書房, 1956, pp.138-44.
[13]辛島驍,『暗号と推理』, 講談社, 1962, pp.246-52.

JOURNAL OF THE SOCIETY OF ARTS

ILLUSTRATION OF PRINCIPLE.



SECRET, OR CYPHER WRITING.

SIR,—Permit me, through the "Journal of the Society of Arts," to make known a system of secret (or cypher) writing I have lately invented and patented the apparatus, and to enclose, for the acceptance of the Society, the apparatus devised for its practical application, which, I believe, will be found to answer all the purposes intended. It is formed, as you perceive, of a series of fixed alphabets printed in *black* letters, and these alternating with another series of double alphabets in *red* letters*; the latter moving in grooves. By this arrangement you can, at pleasure, form any word or words in a line with any letter on the fixed alphabets; for instance, you wish to form the word *telegraph* against K. Begin at the left hand, bringing *T* to the black K, then the next slide move down until *E* is opposite the second black K, and so on until you spell the word, removing the last slide, which is not required. This is the *key-word* to any writing you may wish to send; thus, you desire to communicate the sentence "I have had an interview." Begin by spelling from left to right, using the red letter as the cypher; opposite the *I* you find *R*, the H *B*, A *B*, V *P*, E *A*, H *O*, A *Q*, D *I*, A *X* (then return to the left, and proceed), N *W*, I *C*, N *O*, T *N*, E *A*, R *Y*, V *L*, I *N*, E *B*, W *F*, consequently, the cypher of this message would appear as It B B P A O Q I X W C O N A Y L N B F, which may be read by the party to whom it is sent, by fixing his key word as you did, viz., *telegraph* against K; he reads it by finding the first letter on the red alphabet, and using the black end against it, and so on. It will be seen that, even in this short message, the letter A is represented by *B*, *Q*, and *X*. *B* also represents H, A, and E. I, again, is represented by R, C, and N, and thus leaves no clue to the deciphering, which I feel certain is impossible unless the key-word is known. The same sentence written in the key of *microscope* against U would appear thus:—*A*, *V*, *I*, *S*, *Y*, *F*, *I*, *X*, *B*, *X*, *A*, *B*, *V*, *B*, *L T*, *Q*, *Y*, *R*; in this three *B*'s are together, representing N T E. You may thus vary your cypher *ad infinitum*, and each variation equally unable to be deciphered without the key, but with it is as equally easy. It must be at once apparent that the complexity may be much increased by permutating (on well-known principles) each of the moveable alphabets, and in many other ways; but, in its simplest form, which I have described, I believe it will be found as complete as need be. Of course, the reading and writing may be indifferently from the fixed to the moveable, or the contrary, from left to right, or

* The red letters are here represented by the capitals in italics. Of the four examples which Mr. Thwaites refers to, it has been considered necessary to illustrate only one.

253

Figure 6o. Mr. Thwaites' cipher. Courtesy the Royal Society of Arts.

図1　スゥエーツによる暗号

Soft, sir, one word more,
They are both in either's powers: but this swift business
I must uneasy make, lest too light winning
Make the prize light. One word more I charge thee
That thou attend me, thou dost here usurp
Upon this island as a spy, to win it
From me, the lord on't

図2　シェークスピア『テンペスト』原文(第1幕第2場)

UTMU, DQV, UKS, LKZT, LRWN, FLHL, HPG, SVUS, QR,
KFHWAZI, ORBNDW, EHA, RJZZ, THQJZ, YIHEVURV, N,
VGWW, HUCCJF, NLSI, RBGI, PWE, KLLQF, ALAUGPX,
TBVM, XNB, DGEHU, KLLQU, SQR, DMTU, TPCM, M,
IEOGCM, JGHJ, CTEW, GOMW, RAUPVH, SB, HWKC, TNVY,
QQVH, HZSTG, BQZV, XNFG, XOTQMG, FB, M, WSL, AM,
YZU, JE, NVUJ, AT, PPU, KRWM, AR'W

図3　『テンペスト』原文に対するスゥエーツによる暗号文[*21]

Jexe wii hdx ivow lquq nnka wes vmge fx wadgzjh oxqhow ugp svrg
vwmfi hrzqdmjj a sfwp reclez znfe eqkx dwm mekrg xfxxald xkrh mxh
itpvw ugtzy ybe ruig egzt fsdxtev wlxm kkng xquq sdlisp ci gexs tsaq
iwmh pedon zraa focv gqxdrs xu q cab ry lsx hw fkqp zz gnh lyrh wjk

図4　『テンペスト』原文に対するバベッジによる暗号文

*21 前述したように、バベッジは書簡の中で、この暗号文の2文字目Tが誤りであり、Fが正しいことを指摘している。Ch. Babbage, "Correspondence on Cypher Writing", *Journal of Society of Arts*, No.98, 1854, p.777

文字目	第1の表	第2の表
1	1	1
2	2	2
3	3	3
4	1	4
5	2	5
6	3	6
7	1	7
8	2	8
9	3	1
10	1	2
11	2	3
12	3	4
13	1	5
14	2	6
15	3	7
16	1	8
17	2	1
18	3	2
19	1	3
20	2	4
21	3	5
22	1	6
23	2	7
24	3	8

文字目	使用する表	
1	1	1
2	2	2
3	3	3
4	1	4
5	2	5
6	3	6
7	1	7
8	2	8
9	3	1
10	1	2
11	2	3
12	3	4
13	1	5
14	2	6
15	3	7
16	1	8
17	2	1
18	3	2
19	1	3
20	2	4
21	3	5
22	1	6
23	2	7
24	3	8

左表の関係では、平文から暗号文へは次のように変換されている。
1文字目　S→U
9文字目　N→K
17文字目　R→W

右表の関係では、平文から暗号文へは次のように変換されている。
1文字目　S→U
4文字目　T→U
7文字目　R→V
10文字目　E→S
13文字目　R→Z
16文字目　O→R
19文字目　T→P
22文字目　Y→L

表2　第1の単語を3文字、第2の単語を8文字とした変換表の組み合わせ

	第1の表の1番目の表	第1の表の2番目の表	第1の表の3番目の表
A	c	f	x
B	d	g	y
C	e	h	z
D	f	i	a
E	g	j	b
F	h	k	c
G	i	l	d
H	j	m	e
I	k	n	f
J	l	o	g
K	m	p	h
L	n	q	i
M	o	r	j
N	p	s	k
O	q	t	l
P	r	u	m
Q	s	v	n
R	t	w	o
S	u	x	p
T	v	y	q
U	w	z	r
V	x	a	s
W	y	b	t
X	z	c	u
Y	a	d	v
Z	b	e	w

表3　3文字単語による変換

	第2の表の1番目の表	第2の表の2番目の表	第2の表の3番目の表	第2の表の4番目の表	第2の表の5番目の表	第2の表の6番目の表	第2の表の7番目の表	第2の表の8番目の表
A	c	o	m	b	i	n	e	d
B	d	p	n	c	j	o	f	e
C	e	q	o	d	k	p	g	f
D	f	r	p	e	l	q	h	g
E	g	s	q	f	m	r	i	h
F	h	t	r	g	n	s	j	i
G	i	u	s	h	o	t	k	j
H	j	v	t	i	p	u	l	k
I	k	w	u	j	q	v	m	l
J	l	x	v	k	r	w	n	m
K	m	y	w	l	s	x	o	n
L	n	z	x	m	t	y	p	o
M	o	a	y	n	u	z	q	p
N	p	b	z	o	v	a	r	q
O	q	c	a	p	w	b	s	r
P	r	d	b	q	x	c	t	s
Q	s	e	c	r	y	d	u	t
R	t	f	d	s	z	e	v	u
S	u	g	e	t	a	f	w	v
T	v	h	f	u	b	g	x	w
U	w	i	g	v	c	h	y	x
V	x	j	h	w	d	i	z	y
W	y	k	i	x	e	j	a	z
X	z	l	j	y	f	k	b	a
Y	a	m	k	z	g	l	c	b
Z	b	n	l	a	h	m	d	c

表4　3文字単語による変換

ここでは、Sは表3でuに変換され、
さらに表4でwに変換される。

TWO(*against s*)

	1	2	3
A	b	e	w
B	c	f	x
C	d	g	y
D	e	h	z
E	f	i	a
F	g	j	b
G	h	k	c
H	i	l	d
I	j	m	e
J	k	n	f
K	l	o	g
L	m	p	h
M	n	q	i
N	o	r	j
O	p	s	k
P	q	t	l
Q	r	u	m
R	s	v	n
S	t	w	o
T	u	x	p
U	v	y	q
V	w	z	r
W	x	a	s
X	y	b	t
Y	z	c	u
Z	a	d	v

COMBINED(*against b*)

	1	2	3	4	5	6	7	8
A	b	n	l	a	h	m	d	c
B	c	o	m	b	i	n	e	d
C	d	p	n	c	j	o	f	e
D	e	q	o	d	k	p	g	f
E	f	r	p	e	l	q	h	g
F	g	s	q	f	m	r	i	h
G	h	t	r	g	n	s	j	i
H	i	u	s	h	o	t	k	j
I	j	v	t	i	p	u	l	k
J	k	w	u	j	q	v	m	l
K	l	x	v	k	r	w	n	m
L	m	y	w	l	s	x	o	n
M	n	z	x	m	t	y	p	o
N	o	a	y	n	u	z	q	p
O	p	b	z	o	v	a	r	q
P	q	c	a	p	w	b	s	r
Q	r	d	b	q	x	c	t	s
R	s	e	c	r	y	d	u	t
S	t	f	d	s	z	e	v	u
T	u	g	e	t	a	f	w	v
U	v	h	f	u	b	g	x	w
V	w	i	g	v	c	h	y	x
W	x	j	h	w	d	i	z	y
X	y	k	i	x	e	j	a	z
Y	z	l	j	y	f	k	b	a
Z	a	m	k	z	g	l	c	b

文字	左表	右表	合計
1	1	1	2
2	4	13	17
3	22	11	7
4	1	0	1
5	4	7	11
6	22	12	8
7	1	3	4
8	4	2	6
9	22	1	23
10	1	13	14
11	4	11	15
12	22	0	22
13	1	7	8
14	4	12	16
15	22	3	25
16	1	2	3
17	4	1	5
18	22	13	9
19	1	11	12
20	4	0	4
21	22	7	3
22	1	12	13
23	4	3	7
24	22	2	24

表5　twoとcombinedを用いた変換表(その1)

TWO(*against p*)

	1	2	3
A	e	h	z
B	f	i	a
C	g	j	b
D	h	k	c
E	i	l	d
F	j	m	e
G	k	n	f
H	l	o	g
I	m	p	h
J	n	q	i
K	o	r	j
L	p	s	k
M	q	t	l
N	r	u	m
O	s	v	n
P	t	w	o
Q	u	x	p
R	v	y	q
S	w	z	r
T	x	a	s
U	y	b	t
V	z	c	u
W	a	d	v
X	b	e	w
Y	c	f	x
Z	d	g	y

COMBINED(*against e*)

	1	2	3	4	5	6	7	8
A	y	k	i	x	e	j	a	z
B	z	l	j	y	f	k	b	a
C	a	m	k	z	g	l	c	b
D	b	n	l	a	h	m	d	c
E	c	o	m	b	i	n	e	d
F	d	p	n	c	j	o	f	e
G	e	q	o	d	k	p	g	f
H	f	r	p	e	l	q	h	g
I	g	s	q	f	m	r	i	h
J	h	t	r	g	n	s	j	i
K	i	u	s	h	o	t	k	j
L	j	v	t	i	p	u	l	k
M	k	w	u	j	q	v	m	l
N	l	x	v	k	r	w	n	m
O	m	y	w	l	s	x	o	n
P	n	z	x	m	t	y	p	o
Q	o	a	y	n	u	z	q	p
R	p	b	z	o	v	a	r	q
S	q	c	a	p	w	b	s	r
T	r	d	b	q	x	c	t	s
U	s	e	c	r	y	d	u	t
V	t	f	d	s	z	e	v	u
W	u	g	e	t	a	f	w	v
X	v	h	f	u	b	g	x	w
Y	w	i	g	v	c	h	y	x
Z	x	j	h	w	d	i	z	y

文字	左表	右表	合計
1	4	24	2
2	7	10	17
3	25	8	7
4	4	23	1
5	7	4	11
6	25	9	8
7	4	0	4
8	7	25	6
9	25	24	23
10	4	10	14
11	7	8	15
12	25	23	22
13	4	4	8
14	7	9	16
15	25	0	25
16	4	25	3
17	7	24	5
18	25	10	9
19	4	8	12
20	7	23	4
21	25	4	3
22	4	9	13
23	7	0	7
24	25	25	24

表6　twoとcombinedを用いた変換表(その2)